Application of Probabilistic Risk Assessment (PRA) During Conceptual Design for the NASA Orbital Space Plane (OSP)

James H. Rogers and Fayssal M. Safie, Ph.D.
National Aeronautics and Space Administration
Marshall Space Flight Center
Huntsville, Alabama 35812, USA

James E. Stott and Yunnhon Lo, Ph.D.
Hernandez Engineering, Inc.
Marshall Space Flight Center
Huntsville, Alabama 35812, USA

Abstract

In order to meet the space transportation needs for a new century, America's National Aeronautics and Space Administration (NASA) has implemented an Integrated Space Transportation Plan to produce safe, economical, and reliable access to space. One near term objective of this initiative is the design and development of a next-generation vehicle and launch system that will transport crew and cargo to and from the International Space Station (ISS), the Orbital Space Plane (OSP). The OSP system is composed of a manned launch vehicle by an existing Evolved Expendable Launch Vehicle (EELV). The OSP will provide emergency crew rescue from the ISS by 2008, and provide crew and limited cargo transfer to and from the ISS by 2012. A key requirement is for the OSP to be safer and more reliable than the Soyuz and Space Shuttle, which currently provide these capabilities.

NASA has taken an integrated systems approach in designing the OSP launch system and related ground operations and launch support services. This "System-Centric" approach, as opposed to a "Vehicle-Centric" approach, presents unique challenges in terms of meeting the desired safety and reliability requirements As a result, NASA is utilizing PRA, a methodology for quantitative risk assessment, on the entire

system during the design process and throughout the life of the system. When PRA is performed early in the design and development cycle with full engineering design and operations involvement, the PRA based integrated system model will provide a means for methodical and objective optimisation of the conceptual design.

This paper discusses the development and implementation of PRA in the OSP Program. The OSP Program is the first major NASA program to perform and use PRA during the concept formulation phase of the program and is expected to produce the paradigm by which future space launch systems can be designed to meet successively higher safety and reliability demands [1].

1 Introduction

The Orbital Space Plane (OSP) is a derivative of the former Second Generation Reusable Launch Vehicle (2GRLV) Program. Although called an Orbital Space "Plane," the vehicle conceptual designs represent a variety of shapes. The OSP vehicle will be launched on an existing Evolved Expendable Launch Vehicle (EELV) such as the Atlas V or Delta IV. It is NASA's near term solution to field a new asset for assured U.S. access to and from the International Space Station (ISS) and low-Earth orbit. The OSP will not replace the Space Shuttle fleet, but will serve to complement it and to provide flexibility in operations. The OSP will carry at least four crewmembers. It will provide crew rescue from ISS as soon as practical, but no later than 2008, and crew/cargo transfer to and from ISS by 2012. This will leave the Space Shuttle to ferry large cargo to and from space, to complete the ISS construction, to service the Hubble Space Telescope and to rescue or repair satellites. The intent of the OSP Program is not just development of the vehicle, but the entire system, including ground operations and all supporting technologies needed to conduct missions to and from the ISS.

1.1 OSP Safety Requirements [2,3]

The OSP program has imposed quantitative Safety and Availability design requirements (Table 1), a paradigm shift from the Space Shuttle program. This paradigm shift is generating a change in how space flight system design is approached. The quantitative requirements for Loss of Crew (LOC) are distinct for the two vehicle types, the Crew Rescue Vehicle (CRV) and the Crew Transfer Vehicle (CTV). The CTV LOC risk is during all mission phases from Crew Ingress to Landing/Crew Egress. The CRV LOC risk is from ISS Docking Proximity Operations through Undocking to Landing/Crew Egress. For both requirements,

"crew" is defined as both the occupants of the OSP, as well as occupants of the ISS. That is, if a failure occurred on the OSP during the ISS mated phase and caused a loss of ISS crew, the risk will be accounted for by the OSP. LOC risk due to abort failures and external sources, such as Micrometeoroid and Orbital Debris (M/OD), are included for both vehicle types. In addition to the LOC requirement, the CRV is also subject to an availability requirement of 95% while docked with the ISS with little or no vehicle maintenance.

Crew Rescue Vehicle		
	Objective	Minimum Threshold
Availability	95% with 90% confidence	95% with 50% confidence
Loss of Crew	1/800 with 80% confidence	1/800 with 50% confidence
Crew Transfer Vehicle		
	Objective	Minimum Threshold
Loss of Crew	1/400 with 80% confidence	1/400 with 50% confidence

Table 1. NASA OSP Safety and Availability Requirements

1.2 Integrated RMS Approach

To support the OSP safety requirement, NASA is utilizing an integrated Reliability, Maintainability, and Supportability (RMS) approach (Figure 1). PRA is used because it is the best tool for probabilistically determining if a particular design can meet the safety requirements. The RMS disciplines, methodologies, and processes have been extensively used in an integrated manner by the aerospace industry and by the U.S. Department of Defense for decades. NASA has been slow in implementing this integrated RMS approach, and the OSP Program is the first large-scale program to do so. It will also be the first large-scale space flight system that utilizes PRA in every step of its design process in conjunction with other traditional engineering disciplines.

2 PRA Evolution

The PRA process for the OSP Program had its beginnings during NASA's Space Launch Initiative (SLI) also known as the 2GRLV Program. Initially, it was used to support the conceptual design process under the Inter Center System Analysis Team (ISAT) during the Initial Assessment of Technology Requirements (IATR). But after the reformation of SLI into the OSP and the Next Generation Launch Technologies (NGLT) Programs, the process was then used to support the OSP Requirements Analysis Cycles (RAC) studies.

2.1 ISAT

The ISAT assessment process was performed in three steps: Technology Impact Definition, Advanced Engineering Environment (AEE) Facilitated Architecture Assessment, and Technology Critique.

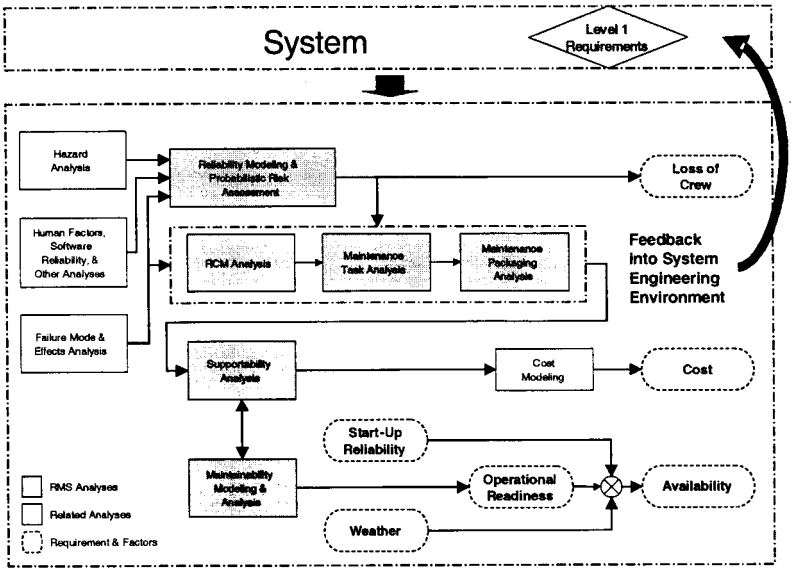

Figure 1. Integrated OSP RMS Process.

2.1.1 Technology Impact Definition

The Technology Impact Definition step was performed by assigning teams to research each technology. After consulting experts and modifying technology models, the teams then passed on their results for input into the AEE.

2.1.2 AEE Facilitated Architecture Assessment

The first step of the AEE process began by defining the vehicle type to be used, the mission to be performed, and the technologies to be implemented in a particular process run. Once vehicle sizing and trajectory analysis were completed, the results were made available for the safety and reliability assessment. The results were then entered into reliability, cost, and operations models. Lastly, the results from all the models were entered into the technology management summary.

2.1.3 Technology Critique

In the management summary, the top-level model results were compared to the reference case for each technology. The participants reviewed the results and judged the credibility of the findings. The analyst investigated any deviations from expected results in order to explain those results. These were then reported to the 2GRLV Program Office, which used the results to direct the next technology assessment.

2.2 RAC Studies

The Requirements Analysis Cycles (RAC) were part of the OSP Analysis and Trade Studies Feasibility Assessment. The RAC intended to show the feasibility of the OSP Level 1 and Level 2 Requirements against natural physical constraints, state of the art as it applies to the program, and all other absolute constraints applying to the project. This is in order to provide program management with the technical foundation to support Program milestones and reviews, Program decisions, requirements validation, technical evaluation of contractor work, and the education and development of the NASA workforce ("smart buyer").

2.3.1 RAC Process

The RAC assessment process, similar to the ISAT process, comprises three groups: Study Teams, which perform analysis tasks based on requirements, the Horizontal Integration Team (HIT), which manages and integrates the overall OSP analysis and trade studies effort, and the Management Review Team (MRT) which reviews and approves trades and analysis results.

2.3.2 Study Teams, Horizontal Integration Team, and Management Review Team

The Study Teams are Inter-Center, multidisciplinary teams assigned analysis tasks based on requirements levied by the HIT. Status and progress reports are sent to the HIT. Once the analysis is satisfactorily completed, as determined by the HIT, the results are sent to the MRT. The MRT then evaluates the results and either approves or rejects analysis results.

2.3.3 RAC Results

The RAC studies have identified the significant technical discriminators and engineering challenges when assessing the feasibility of a system that meets the Level I and Level II requirements. The teams identified areas for further clarification or re-interpretation of several requirements, including CRV availability, on-orbit maneuverability, launch probability, and contingency cargo. The RAC studies have also identified significant system characteristics that affect the feasibility assessment including, OSP spacecraft hypersonic lift over drag, OSP spacecraft abort and escape modes for both ascent and descent, rapid separation from ISS, autonomous rendezvous and mating with ISS, range safety, OSP/EELV integration, and OSP crew time sensitivity.

3 PRA

3.1 NASA PRA Working Group

The OSP Contractors are encouraged to use PRA as the primary basis for evaluating the compliance of their own concepts to the LOC requirement. The NASA PRA Working Group was formed to facilitate this evaluation, as well as to promote consistency among the contractors' analyses. The PRA working group consists of PRA representatives from selected NASA centers and their support contractors. To ensure unbiased support to the both OSP contractors and full integration with the RMS approach, the interactions with the OSP contractors are through the OSP RMS working group. A strict "Rules of Engagement" is being followed to avoid any impropriety.

3.2 Generic Top-Level Model

The PRA working group was initially tasked to perform a PRA on the NASA OSP design concept derived from NASA's RAC studies. When the program moved into the System Definition Review (SDR) phase, a top-level PRA model template and ground rules and assumptions on a generic, non-architecture specific vehicle were assembled.

The generic top-level model template serves two main purposes. One, to ensure consistency in the modeling among the contractors. Two, to serve as a test problem for the contractor in demonstrating its architecture's capability to meet the quantitative requirements. Each contractor is also encouraged to use PRA in its design process. PRA can help in identifying the combination of events, failures and other conditions that pose a risk to the system. Its probabilistic nature facilitates the ranking of the risks, allowing the design and management teams to focus resources on the most significant risks and on developing risk reduction strategies at the engineering design and operational planning levels.

3.3 OSP PRA Process [4]

The OSP PRA development process will follow the general PRA guidelines as presented in the NASA PRA Guidelines. This process takes the form of the event tree with fault tree linking approach, beginning with the identification (via a functional master logic diagram) of "initiating events" that perturb the system. For each initiating event, the analysis proceeds by determining the additional failures that may lead to undesirable consequences. Then, the consequences of these scenarios are determined, as well as their frequencies. Finally, the scenarios are gathered to create the risk profile of the system using Monte Carlo simulation.

The PRA will focus on identifying and understanding the design, operational characteristics, and performance of the concepts under evaluation that drive the differences in risk among them. More detailed models may be developed as necessary to conduct specific trades. After system down-select the level of modeling detail will mimic the level of design down to the point were design and operational trades may continue to be meaningful supported.

Because the initial PRA addresses the conceptual design of alternate configurations prior to SDR, the process for this effort will emphasize functional analysis. Taking a functional approach will permit a meaningful comparison of these concepts in terms of their compliance with the safety requirements and the varying approaches and system configurations utilized in providing the functions. Where specific failure data is not available for that subsystem quantification may be done via 'similarity' analysis. Similarity analysis uses data from similar subsystems or components to generate failure distributions for the subsystem or component of interest.

During operation there are many questions related to the anticipated success of the program or mission. The PRA will serve to predict impacts to the OSP program that could be detrimental to success. For operations the PRA will focus on aspects of risk that relate to the operation of the system or performance of the mission. Risk importance measures determined by the PRA will be used to optimize resource allocations during operations. The PRA will also be used to evaluate flight readiness by quantifying the risk impact caused by a nonconformance to system specifications.

After the system has been operational and experience has been gained, improvements may be required. Changing technology, obsolescence of some components and aging will play a significant role in the needs for improvement or upgrade of a mature OSP system. To this end, the PRA will be used to evaluate and rank options for upgrades that reduce risk. PRA provides a consistent assessment tool in evaluating the risk benefits of alternative upgrades.

4 Conclusion

NASA has taken an innovative approach to safety and reliability on the OSP Program. An approach that is based on a well-defined systems engineering process, which, for the first time includes quantitative safety and reliability measures at the conceptual stage as part of system trades. Using an integrated systems engineering process, NASA's OSP program is able to perform trades to identify architectures that meet its performance requirements while maximizing safety. This innovative approach provides the pathway to a risk based process that promises to achieve NASA's goal of improving safety. Achievement of this goal should greatly enhance the prospects for manned space flight in the future.

References

1. NASA. Orbital Space Plane Fact Sheet: Beginning a New Era of Space Flight: The Orbital Space Plane. FS-2003-05-64-MSFC, May 2003
2. NASA. Orbital Space Plane Level II System Requirements Document. MSFC-RQMT-3360, Nov 2003
3. NASA. Orbital Space Plane Level I Requirements Program Interpretation Document. OSP-DOC-001, Nov 2003
4. NASA. Probabilistic Risk Assessment Procedures Guide for NASA Mangers and Practitioners. Pending Approval, Aug 2002